Searching PAJ

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-158650
(43)Date of publication of application : 31.05.2002

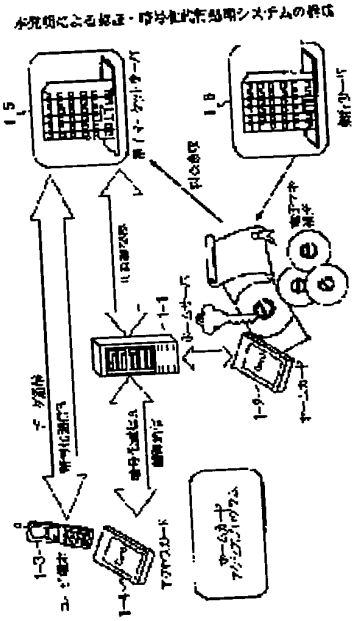
(51)Int.Cl. H04L 9/08
G06K 19/00
G09C 1/00
H04L 9/32

(21)Application number : 2000-353895
(22)Date of filing : 21.11.2000

(71)Applicant : FUJITSU LTD
(72)Inventor : AKAMA KATSUAKI

(54) PROXY SERVER FOR CERTIFICATION/CIPHERING PROCESSING, ACCESS CARD PROGRAM RECORDING MEDIUM AND PORTABLE TERMINAL

(57)Abstract:
PROBLEM TO BE SOLVED: To accelerate certification/encoding processing and to conveniently and safely perform electronic commerce, etc., regarding a proxy server for certification/encoding processings to act for encoding and certification processings of communication information in the electronic commerce, etc., in place of a user terminal and an access card to enable access to the server.
SOLUTION: A home card 1-2, connected with a home server 1-1 provided at home, etc., is provided with a function to act for a preprocessing of encoding communication, including certification and replacement of common keys in the electronic commerce, etc., with an electronic market server 1-5; the home server 1-1 is accessed from the user terminal 1-3 carried by a user by using the access card 1-4; the preprocessing of the encoding communication including the certification and the replacement of the common keys is performed at high speed by the home server 1-1; the common key obtained by the preprocessing is notified to the user terminal 1-3 and the user terminal 1-3 distributes information of the electronic commerce, etc., by using the common key.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－158650
(P2002－158650A)
(43)公開日　平成14年５月31日(2002.5.31)

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
H04L 9/08		G09C 1/00	640B 5B035
G06K 19/00			640Z 5J104
G09C 1/00	640	H04L 9/00	601C
		G06K 19/00	Q
H04L 9/32		H04L 9/00	601A

審査請求　未請求　請求項の数10　ＯＬ　（全 25 頁）　最終頁に続く

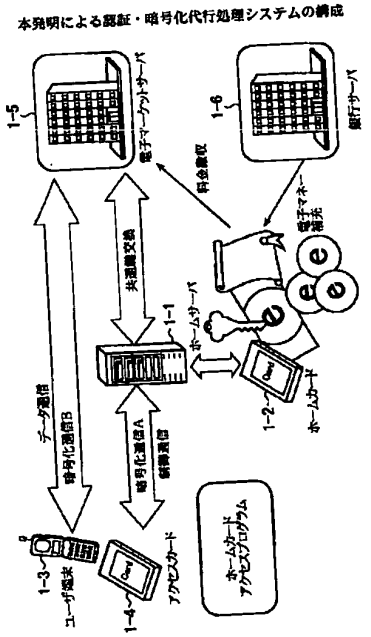
(21)出願番号　特願2000－353895(P2000－353895)
(22)出願日　平成12年11月21日(2000.11.21)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　赤間　勝明
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100105337
弁理士　眞鍋　潔　（外３名）

Ｆターム(参考)　5B035 AA13 BB09 BC03 CA11
5J104 AA01 AA07 AA09 AA16 AA18
EA06 EA19 JA03 KA02 NA02
NA12 NA20 NA35 NA37 NA38
NA40 PA12

(54)【発明の名称】　認証・暗号化処理代行用のサーバ、アクセスカード、プログラム記録媒体及び携帯端末

(57)【要約】
【課題】　電子商取引等における通信情報の暗号化及び認証処理を、ユーザ端末機器に代わって代行する認証・暗号化処理代行サーバ及び該サーバへのアクセスを許可するアクセスカードに関し、認証・暗号化処理の高速化を図り、且つ、電子商取引等を簡便に安全に行えるようにする。
【解決手段】　家庭内等に備えたホームサーバ１－１に接続したホームカード１－２に、電子マーケットサーバ１－５との電子商取引等における認証及び共通鍵の交換を含む暗号化通信の前処理を代行する機能を具備させ、ユーザが携帯するユーザ端末機器１－３からアクセスカード１－４を用いてホームサーバ１－１にアクセスし、ホームサーバ１－１により、認証及び共通鍵の交換を含む暗号化通信の前処理を高速に行い、該前処理により得られた共通鍵をユーザ端末機器１－３に通知し、ユーザ端末機器１－３は該共通鍵を用いて電子商取引等の情報流通を行う。



1

【特許請求の範囲】

【請求項１】　ユーザ端末機器からアクセスされ、該アクセスの際に送信される電子署名を確認し、該ユーザ端末機器との間で暗号化された通信セッションを確立する手段を備えたサーバであって、

公開鍵及び秘密鍵を用い、認証処理を経て共通鍵を交換し、該共通鍵により暗号化通信を行う電子マーケットサーバ等の他のサーバに対して、該認証処理及び共通鍵の交換処理を、前記ユーザ端末機器に代わって行う認証・暗号化処理代行手段と、

前記電子マーケットサーバ等の他のサーバと交換した共通鍵を、前記ユーザ端末機器に暗号化された通信セッションを介して通知する手段と、

を備えたことを特徴とすると認証・暗号化処理代行サーバ。

【請求項２】　前記認証・暗号化処理代行サーバは、電子商取引を行うための電子署名機能及び認証機能を含む暗号化管理手段を備えたホームカードを格納し、前記電子マーケットサーバ等の他のサーバに対する認証処理及び共通鍵の交換処理を、該ホームカードの暗号化管理手段により実行することを特徴とする請求項１に記載の認証・暗号化処理代行サーバ。

【請求項３】　前記ホームカードは、前記ユーザ端末機器からの第１のパスワード入力によりアクセスを可能にする論理回路を備え、該アクセスを許可したユーザ端末機器との間に暗号化された通信セッションを確立した後に、該ユーザ端末機器から入力される第２のパスワードにより、前記認証・暗号化処理代行手段のセキュリティを解放する手段を備えたことを特徴とする請求項２に記載の認証・暗号化処理代行サーバ。

【請求項４】　前記ホームカードは、該ホームカード内の電子マネーにより決済された決裁情報を記録し、該記録した決済情報を所定のメールアドレス宛てに通知する手段を備えたことを特徴とする請求項２に記載の認証・暗号化処理代行サーバ。

【請求項５】　前記ホームカードは、該ホームカード内の電子マネーによる決済処理に対して、該決済処理の取り消しの認証情報に基づいて該決裁情報を取り消すと共に、該決済処理により減算された電子マネーを、ホームカード内の電子マネーに加算する手段を備えたことを特徴とする請求項４に記載の認証・暗号化処理代行サーバ。

【請求項６】　前記ホームカードは、前記ユーザ端末機器から要求された電子マネーの再補充要求に対して、銀行サーバ等の電子マネー管理サーバの認証情報に基づいて、要求された補充額を該ホームカードの電子マネーに加算し、再補充する手段を備えたことを特徴とする請求項２に記載の認証・暗号化処理代行サーバ。

【請求項７】　ユーザ端末機器に接続されるアクセスカードであって、認証・暗号化処理代行機能を備えたサーバとの間に、暗号化された通信セッションを確立する手段と、

2

前記認証・暗号化処理代行機能を備えたサーバが電子マーケットサーバ等の他のサーバに対して認証処理後に交換した共通鍵を、前記暗号化された通信セッションを介して受信し、該受信した共通鍵を用いて該電子マーケットサーバ等の他のサーバとの暗号化通信を行う手段と、

を備えたことを特徴とするアクセスカード。

【請求項８】　携帯端末の認証を該携帯端末との間で所定の手順に従った通信により行う認証機能を備えた種々のサーバと通信可能なサーバにおいて、

該携帯端末から該携帯端末の識別情報及び認証代行処理依頼信号を受信する受信手段と、

該識別情報が内部メモリ又は外部メモリに記憶されているか否か判定する判定手段と、

前記判定によりメモリに記憶されている場合に、前記所定の手順に従った通信の一部又は全部を該携帯端末に代わって行う代行手段と、

を備えたことを特徴とするサーバ。

【請求項９】　携帯端末の認証を該携帯端末との間で所定の手順に従った通信により行う認証機能を備えた種々のサーバと通信可能なサーバ用のプログラムを記憶した記録媒体において、

該携帯端末から該携帯端末の識別情報及び認証代行処理依頼信号を受信するステップと、

該識別情報が内部メモリ又は外部メモリに記憶されているか否か判定するステップと、

前記判定によりメモリに記憶されている場合に、前記通信の一部又は全部を該携帯端末に代わって行うステップと、

をサーバが実行するためのプログラムを記憶した記録媒体。

【請求項１０】　所定の手順に従った通信により通信相手の認証を行い、認証の結果、正当な通信相手であると判定した場合に、該通信相手との暗号化通信を行う際に使用する秘密情報を、該通信相手に対して送信する機能を備えた種々のサーバと通信可能な携帯端末において、

自端末の識別情報及び認証代行処理依頼信号を所定のサーバに対して送信する送信手段と、

該所定のサーバが該携帯端末に代わって前記所定の手順に従った通信を行い、取得した秘密情報を、該所定のサーバから受信する受信手段と、

を備えたことを特徴とする携帯端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、認証・暗号化処理代行サーバ及びアクセスカードに関し、より詳しくは、電子商取引における発注や決済等に伴う通信情報の暗号化及び認証処理を、ユーザ端末機器に代わって行う認証・暗号化処理代行サーバ及び該サーバへのアクセスを許

可するアクセスカードに関する。

【０００２】電子商取引などのように、個人情報又は秘密情報の通信を伴う情報の流通においては、それらの情報が盗用されたり、不正使用されたり、或いは改ざんされたりすることなく、安全に通信相手との間で送受されるよう、通信情報のセキュリティを確保することが重要であり、通信情報のセキュリティを確保するための処理手順には高い信頼性が要求されるが、電子商取引などを利用するユーザに対しては、操作が簡便で且つ、セキュリティ確保のための処理が短時間で完了することが要請される。

【０００３】電子商取引等の情報流通には、種々のユーザ端末機器が利用され、また、ユーザは電子商取引等の情報流通を様々な場所で行えることが望ましい。図２５は電子商取引等における情報流通に使用されるユーザ端末機器及び情報処理装置の例を示している。

【０００４】２５－１はデータ通信機能や個人情報管理用ソフトウェア（ＰＩＭ：personalinformation manager）等を組込んだ無線携帯電話機、２５－２は携帯情報端末（ＰＤＡ：personal digital assistants）、２５－３は有線多機能電話端末、２５－４はインターネットに接続されるパーソナルコンピュータ、２５－５はＩＣカード等を利用可能な公衆電話機、２５－６は商店や事務所等のデスクトップ型データ処理装置、２５－７は銀行業務用のサーバ、２５－８は信販会社用のサーバ、２５－９は電子マーケットサーバである。

【０００５】ユーザは上記ユーザ用の端末機器２５－１～２５－６の何れかを使用し、電子商取引用のサーバ２５－１０を介して電子マーケットサーバ２５－９に接続し、暗号化技術、電子署名技術、認証技術等の通信情報セキュリティ技術を用いて電子商取引等の情報流通を行う。

【０００６】

【従来の技術】図２６に従来の電子商取引等におけるセキュリティ管理技術を示す。従来のセキュリティ管理は、電子商取引等を行うユーザのユーザ端末機器２６－１と電子マーケットサーバ２６－２との間で、ｈｔｔｐｓ（hypertext transfer protocol over transport layer security / secure sockets layer）等のセキュリティ機能を有するプロトコルによるセッションを介して、認証及び注文の受付け等に関する暗号化通信を行い、電子マーケットサーバ２６－２は、該電子商取引等に係る決済処理を信販会社用のサーバ２６－３に対して行い、信販会社用のサーバ２６－３は銀行業務用のサーバ２６－４に対して決済処理を行う。

【０００７】図２７は上記従来のセキュリティ管理の通信手順を示す。先ず、ユーザ端末機器２６－１は、電子マーケットサーバ２６－２に対し、ｈｔｔｐｓプロトコルによるセキュリティ確保のセッション要求を送信する（ステップ２７－１）。ここで、ユーザ端末機器２６－１は、自己の公開鍵Ｋｕ及びその対となる秘密鍵Ｓｕを保有し、電子マーケットサーバ２６－２は、自己の公開鍵Ｋｓ及びその対となる秘密鍵Ｓｓを保有しているものとする。

【０００８】電子マーケットサーバ２６－２は、上記セキュリティ確保のセッション要求（ｈｔｔｐｓ：／／）を受信すると、ユーザ端末機器２６－１に対して、乱数“ａ”及び該電子マーケットサーバ２６－２が正規の真正なサーバであることを証明するサーバ証明書を送信する（ステップ２７－２）。該サーバ証明書は約２キロバイトの長さを有し、その中には、電子マーケットサーバ２６－２の公開鍵Ｋｓ及び該証明書発行元の認証局（ＣＡ：certificate authority）情報等が含まれている。

【０００９】ユーザ端末機器２６－１はサーバ証明書を受信すると、該サーバ証明書が真正なものであるかを確認するために、該証明書の発行元の認証局（ＣＡ）に検証要求を送信する（ステップ２７－３）。認証局（ＣＡ）は該要求に対して該サーバ証明書を検証し、真正なものであれば、その旨の認証をユーザ端末機器２６－１に送信する（ステップ２７－４）。

【００１０】ユーザ端末機器２６－１は電子マーケットサーバ２６－２の認証を得た後、電子マーケットサーバ２６－２に対して、クライアント証明書を送信する（ステップ２７－５）。このクライアント証明書は約２キロバイトの長さを有し、その中にはユーザ端末機器２６－１の公開鍵Ｋｕ及び該証明書発行元認証局（ＣＡ）情報等が含まれている。

【００１１】電子マーケットサーバ２６－２は、クライアント証明書を受信すると、該クライアント証明書が真正なものであるかを確認するために、該証明書の発行元の認証局（ＣＡ）に検証要求を送信する（ステップ２７－６）。認証局（ＣＡ）は該要求に対して該クライアント証明書を検証し、真正なものであればその旨の認証を電子マーケットサーバ２６－２に送信する（ステップ２７－７）。

【００１２】電子マーケットサーバ２６－２は、ユーザ端末機器２６－１の認証を得た後、ユーザ端末機器２６－１に対して暗号化していない平文の情報を送信する（ステップ２７－８）。ユーザ端末機器２６－１は、電子マーケットサーバ２６－２から受信した平文の情報を、ユーザ端末機器２６－１の秘密鍵Ｓｕで暗号化した暗号文を、電子マーケットサーバ２６－２に送り返す（ステップ２７－９）。

【００１３】電子マーケットサーバ２６－２は、ユーザ端末機器２６－１の秘密鍵Ｓｕで暗号化され送信された上記暗号文を、先に通知されたユーザ端末機器２６－１の公開鍵Ｋｕにより復号化し、該復号化した情報と、自身が最初に送信した平文情報とを照合することにより、ユーザ端末機器２６－１の署名機能を確認する。以上の公開鍵、秘密鍵を使用した署名機能は、周知のＲＳＡ

5

(Rivest Shamir Adleman) のような公開鍵暗号方式に基づいて行われている。

【００１４】電子マーケットサーバ２６－２は、ユーザ端末機器２６－１の署名機能が確認された後、共通鍵用のマスタ鍵Ｍｋの情報を、電子マーケットサーバ２６－２の秘密鍵Ｓｓで暗号化してユーザ端末機器２６－１に送信する（ステップ２７－１０）。

【００１５】ユーザ端末機器２６－１は、電子マーケットサーバ２６－２から送信された共通鍵用のマスタ鍵Ｍｋの暗号文を、先に通知された電子マーケットサーバ２６－２の公開鍵Ｋｓにより復号化し、復号化したマスタ鍵Ｍｋと先の乱数“ａ”とを組合わせて、共通鍵Ｘを生成する。

【００１６】このような手順を経て、ユーザ端末機器２６－１と電子マーケットサーバ２６－２とで、暗号化及び復号化に共通に使用される共通鍵Ｘが確定し、該共通鍵Ｘを用いて、電子商取引等の情報流通に必要な個人情報や秘密情報の送受が行われる（ステップ２７－１１）。

【００１７】上記の手順は、電子商取引の相手先である電子マーケットサーバが異なれば、それぞれの相手先の電子マーケットサーバに対して、個別に行わなければならない。図２８は複数の電子マーケットと電子商取引を行う様子を示している。

【００１８】ユーザ端末機器２８－１を使用し、或る電子マーケットＡと電子商取引を行い、続いて他の電子マーケットＢと電子商取引を行う場合、ユーザ端末機器２８－１と電子マーケットＡのサーバ２８－２との間で、公開鍵、秘密鍵及び証明書を用いて前述の図２７に示した手順により、共通鍵X_A 交換のための暗号化通信を行って電子商取引を行い、また、他の電子マーケットＢのサーバ２８－３に対しても、全く同様の手順により共通鍵X_B 交換のための暗号化通信を行って電子商取引を行わなければならない。

【００１９】

【発明が解決しようとする課題】電子商取引等における個人情報又は秘密情報及び認証情報の送受に際して、それらのセキュリティ管理のために、公開鍵の授受、証明書の認証による相手確認、公開鍵及び秘密鍵を用いた暗号化通信による電子署名及び共通鍵の交換を行い、これら暗号化通信の前処理を終えてから、電子商取引等を行うための本体情報が共通鍵により暗号化されて送信される。

【００２０】このセキュリティ管理手順において、公開鍵及び秘密鍵を用いた暗号化及び復号化は、多くの演算処理を必要とし、処理能力の低いユーザ端末機器の場合、数秒乃至数十秒の時間が必要となる。また、取引相手同士がお互いに相手の認証を確認するためには、数キロバイト単位の証明書データの交換が必要で、このデータの通信時間が更に加わり、暗号化通信の前処理に数十秒といった多くの時間が掛かり、利用者はその間待ちあぐむことになり、また、その間にも通信料金は課金され、特に、複数の電子マーケットを相手に頻繁に電子商取引を行う場合には、該暗号化通信の前処理である認証・共通鍵交換処理に長い時間が掛かるため、通信料金が嵩んでしまうこととなる。

6

【００２１】また、特に携帯用のユーザ端末機器の紛失又は盗難等に遭った場合、ユーザ端末機器が第三者の手に渡ると、ユーザ端末機器内には、電子商取引に必要な情報（公開鍵、秘密鍵、証明書、電子マネー等）が格納されているため、第三者によりユーザ端末機器内の情報が解析され、不正に利用される危険性がある。

【００２２】本発明は、電子商取引等における個人情報又は秘密情報及び認証情報の送受に際して、それらのセキュリティ管理のために行われる共通鍵の交換を含む暗号化通信の前処理を短時間で行い、ユーザの待ち時間を短縮し、通信料金を節減させ、また、電子商取引等における個人情報又は秘密情報及び認証情報の不正利用に対するセキュリティ性を高めると共に、ユーザ端末機器を用いて電子商取引等が簡便にかつ安全に行えるようにすることを目的とする。

【００２３】

【課題を解決するための手段】上記課題を解決するために本発明は、セキュリティの確保された例えば家庭内に設置されるホーム網用のホームサーバ等のサーバに、電子商取引等における認証及び共通鍵の交換を含む暗号化通信の前処理を代行する機能を具備させ、ユーザが操作するユーザ端末機器からアクセスカードを用いて、該ホームサーバ等の認証・暗号化処理代行サーバにアクセスし、該認証・暗号化処理代行サーバにより、認証及び共通鍵の交換を含む暗号化通信の前処理を高速に行い、該前処理により得られた共通鍵をユーザ端末機器に通知し、ユーザ端末機器は該共通鍵を用いて電子商取引等の情報流通を行い得るようにしたものである。

【００２４】即ち、本発明の認証・暗号化処理代行サーバは、（１）ユーザ端末機器からアクセスされ、該アクセスの際に送信される電子署名を確認し、該ユーザ端末機器との間で暗号化された通信セッションを確立する手段を備えたサーバであって、公開鍵及び秘密鍵を用い、認証処理を経て共通鍵を交換し、該共通鍵により暗号化通信を行う電子マーケットサーバ等の他のサーバに対して、該認証処理及び共通鍵の交換処理を、前記ユーザ端末機器に代わって代行する認証・暗号化処理代行手段と、前記電子マーケットサーバ等の他のサーバと交換した共通鍵を、前記ユーザ端末機器に暗号化された通信セッションを介して通知する手段と、を備えたものである。

【００２５】また、（２）前記認証・暗号化処理代行サーバは、電子商取引を行うための電子署名機能及び認証機能を含む暗号化管理手段を備えたホームカードを格納

し、前記電子マーケットサーバ等の他のサーバに対する認証処理及び共通鍵の交換処理を、該ホームカードの暗号化管理手段により実行するものである。

【００２６】また、（３）前記ホームカードは、前記ユーザ端末機器からの第１のパスワード入力によりアクセスを可能にする論理回路を備え、該アクセスを許可した該ユーザ端末機器との間に暗号化された通信セッションを確立した後に、該ユーザ端末機器から入力される第２のパスワードにより、前記認証代行手段のセキュリティを解放する手段を備えたものである。

【００２７】また、（４）前記ホームカードは、該ホームカード内の電子マネーにより決済された決裁情報を記録し、該記録した決済情報を所定のメールアドレス宛てに通知する手段を備えたものである。

【００２８】また、（５）前記ホームカードは、該ホームカード内の電子マネーによる決済処理に対して、該決済処理の取り消しの認証情報に基づいて該決裁情報を取り消すと共に、該決済処理により減算された電子マネーを、ホームカード内の電子マネーに加算する手段を備えたものである。

【００２９】また、（６）前記ホームカードは、前記ユーザ端末機器から要求された電子マネーの再補充要求に対して、銀行サーバ等の電子マネー管理サーバの認証情報に基づいて、要求された補充額を該ホームカードの電子マネーに加算し、再補充する手段を備えたものである。

【００３０】また、本発明のアクセスカードは、（７）ユーザ端末機器に接続されるアクセスカードであって、認証・暗号化処理代行機能を備えたサーバとの間に、暗号化された通信セッションを確立する手段と、前記認証・暗号化代行機能を備えたサーバが電子マーケットサーバ等の他のサーバに対して認証処理後に交換した共通鍵を、前記暗号化された通信セッションを介して受信し、該受信した共通鍵を用いて該電子マーケットサーバ等の他のサーバとの暗号化通信を行う手段と、を備えたものである。

【００３１】また、本発明のサーバは、（８）携帯端末の認証を該携帯端末との間で所定の手順に従った通信により行う認証機能を備えた種々のサーバと通信可能なサーバにおいて、該携帯端末から該携帯端末の識別情報及び認証代行処理依頼信号を受信する受信手段と、該識別情報が内部メモリ又は外部メモリ（例えば、ホームカード）に記憶されているか否か判定する判定手段と、前記判定によりメモリに記憶されている場合に、前記所定の手順に従った通信の一部又は全部を該携帯端末に代わって行う代行手段と、を備えたものである。

【００３２】また、本発明のプログラムを記憶した記録媒体は、（９）携帯端末の認証を該携帯端末との間で所定の手順に従った通信により行う認証機能を備えた種々のサーバと通信可能なサーバ用のプログラムを記憶した記録媒体において、該携帯端末から該携帯端末の識別情報及び認証代行処理依頼信号を受信するステップと、該識別情報が内部メモリ又は外部メモリに記憶されているか否か判定するステップと、前記判定によりメモリに記憶されている場合に、前記通信の一部又は全部を該携帯端末に代わって行うステップと、をサーバが実行するためのプログラムを記憶したものである。

【００３３】また、本発明の携帯端末は、（１０）所定の手順に従った通信により通信相手の認証を行い、認証の結果、正当な通信相手であると判定した場合に、該通信相手との暗号化通信を行う際に使用する秘密情報を、該通信相手に対して送信する機能を備えた種々のサーバと通信可能な携帯端末において、自端末の識別情報及び認証代行処理依頼信号を所定のサーバに対して送信する送信手段と、該所定のサーバが該携帯端末に代わって前記所定の手順に従った通信を行い、取得した秘密情報を、該所定のサーバから受信する受信手段と、を備えたものである。

【００３４】

【発明の実施の形態】図１に本発明による認証・暗号化代行処理システムの構成を示す。同図において、１－１は電子商取引等を行うユーザのホームサーバ、１－２は該ユーザのホームカード、１－３はユーザ端末機器、１－４はホームカードへのアクセスを可能にするアクセスカード、１－５は電子マーケットサーバ、１－６は銀行業務用サーバである。

【００３５】ホームサーバ１－１は、電子商取引等を行うユーザの家庭内等、秘密情報の管理を安全に行うことができる場所に設置され、且つ、インターネットに接続可能であると共に、ユーザ端末機器１－３からアクセス可能なサーバである。ホームサーバ１－１は、家庭内等において他の電化製品や宅内機器に接続されてホーム網を構成するサーバを利用することができる。なお、ホームサーバ１－１は、各家庭内等に設置する代わりに、秘密情報の管理に信頼を置くことができる特定の機関等に一括して設けたものであってもよい。

【００３６】ホームカード１－２は、電子商取引に使用され、正式な認証用の証明書及び各電子マーケットの公開アルゴリズム等を内蔵するＩＣカードであり、ユーザが書き換え可能なパスワードを判定するハードウェア論理回路を備え、該パスワードの入力によってアクセス可能となる。ホームカード１－２は、セキュリティの確保されたホーム網内でホームサーバ１－１に常時接続されている。

【００３７】アクセスカード１－４は、ユーザ端末機器１－３からホームカード１－２へアクセスするためのカードであり、該アクセスカード１－４内にはホームカードへのアクセスプログラムを格納する。アクセスカード１－４内のホームカードアクセスプログラムにより、ユーザ端末機器１－３とホームカード１－２との間に制御

通信（暗号化通信）が確立される。

【００３８】ホームカード１－２は、パスワードによるセキュリティがハードウェア論理回路によって掛けられており、パスワードの入力によってアクセスが許可されたユーザ端末機器１－３に対して制御通信確立後、更に、ユーザ端末機器１－３からホームカード１－２の機能使用のセキュリティを解放するパスワードを投入することによって、該ホームカード１－２を利用した電子商取引が可能となる。

【００３９】ユーザがユーザ端末機器１－３により電子マーケットサーバ１－５と暗号化通信を行う場合、ホームサーバ１－１が、ホームカード１－２内のセキュリティ情報を用いて、電子マーケットサーバ１－５との間で、認証及び共通鍵交換の処理までを、ユーザ端末機器１－３に代わって高速に実行する。

【００４０】電子マーケットサーバ１－５との共通鍵の交換が終了した時点で、その共通鍵を、制御通信回線を用いて、ユーザ端末機器１－３に通知する（暗号化通信Ａ）。ユーザ端末機器１－３は、その通知された共通鍵を用いて、電子マーケットサーバ１－５と暗号化されたデータ通信を行い（暗号化通信Ｂ）、電子マーケットサーバ１－５との間で個人情報又は秘密情報等を送受するデータ通信を行う。

【００４１】図２に上記本発明による認証・暗号化代行処理手順を示す。ユーザ端末機器１－３とホームサーバ１－１との間では、予め、アクセスカードによって制御通信（暗号化通信）セッションを確立し、以下の手順で共通鍵Ｘ´の交換処理を行っておく。

【００４２】先ず、ユーザ端末機器１－３からアクセスカードによりホームサーバ１－１内のホームカードにアクセスし（ステップ２－１）、ユーザ端末機器１－３とホームサーバ１－１との間に制御通信（暗号化通信）セッションを確立する（ステップ２－２）。そして、ユーザ端末機器１－３は乱数“ｂ”を生成し、該乱数“ｂ”をユーザ端末機器１－３の秘密鍵Ｓｕで暗号化し、該暗号化した乱数“ｂ”とユーザ端末機器１－３の識別情報ＩＤとを、上記制御通信（暗号化通信）セッションによりホームサーバ１－１へ送信し、共通鍵交換を要求する（ステップ２－３）。

【００４３】ホームサーバ１－１は、内部又は外部にアクセス可能に設けたメモリにアクセスし、ユーザ端末機器１－３から受信したユーザ端末機器識別情報ＩＤに対応する公開鍵Ｋｕを読み出し、乱数“ｂ”を復号化すると共に、共通鍵用のマスタ鍵Ｍｋ´を生成し、該マスタ鍵Ｍｋ´と乱数“ｂ”を組合わせて共通鍵Ｘ´を作成する。また、該マスタ鍵Ｍｋ´をホームサーバ１－１の秘密鍵Ｓｈで暗号化し、ユーザ端末機器１－３へ送信する（ステップ２－４）。尚、前記メモリは、代行で認証を行う対象のユーザ端末機器の識別情報とその公開鍵Ｋｕを対応付けて記憶しており、ホームサーバ内又は該サーバと接続される他の装置内に設けられている。

【００４４】ユーザ端末機器１－３は、ホームサーバ１－１から送信されたマスタ鍵Ｍｋ´の暗号文を、ホームサーバ１－１の公開鍵Ｋｈにより復号化し、該復号化したマスタ鍵Ｍｋ´と乱数“ｂ”とを組合わせて共通鍵Ｘ´を生成する。このようにして、ユーザ端末機器１－３とホームサーバ１－１とで、予め共通鍵Ｘ´を取り交わし、それぞれで保管しておく。この共通鍵Ｘ´の交換後、ユーザ端末機器１－３とホームサーバ１－１との間の、制御通信（暗号化通信）セッションは開放される（ステップ２－５）。

【００４５】その後、ユーザがユーザ端末機器１－３を用いて、電子商取引を行う場合、アクセスカード１－４によりホームサーバ１－１にアクセスし、セキュリティ確保のセッション要求（ｈｔｔｐｓ：／／）を送信する（ステップ２－６）。該セキュリティ確保のセッション要求を受信したホームサーバ１－１は、ホームカード１－２内のセキュリティ情報を用い、電子マーケットサーバ１－５との間で、従来の図２７に示す手順と同様の手順で、相互の証明書の認証処理、並びに公開鍵及び秘密鍵による共通鍵Ｘの交換処理を実行する（ステップ２－７）。

【００４６】ホームサーバ１－１は固定設置の大型装置であるため、ユーザ端末機器１－３に比べて、演算処理速度や通信処理速度等が速く、高いデータ処理能力を有し、上記共通鍵Ｘの交換までの処理を、ユーザ端末機器１－３で行った場合に比べて高速に実行する。

【００４７】そして、電子マーケットサーバ１－５との間で交換した共通鍵Ｘの情報を、前述のユーザ端末機器１－３とホームサーバ１－１との間で交換した共通鍵Ｘ´を用いて暗号化し、ユーザ端末機器１－３へ送信する（ステップ２－８）。ユーザ端末機器１－３は、該共通鍵Ｘの情報の暗号文を解読し、共通鍵Ｘの情報を得、以降、該共通鍵Ｘを用いて電子マーケットサーバ１－５との間で、電子商取引等に関する情報の暗号化通信を行う（ステップ２－９）。

【００４８】なお、前述の手順において、ホームサーバ１－１から共通鍵Ｘをユーザ端末機器１－３へ通知せずに、ホームサーバが電子マーケットサーバとの暗号化通信を共通鍵Ｘにより解読し、該解読した通信文を共通鍵Ｘ´で暗号化してユーザ端末機器に送信し、また、ユーザ端末機器から共通鍵Ｘ´で暗号化された暗号文を解読し、該解読した通信文を共通鍵Ｘで暗号化して電子マーケットサーバへ送信するようにしもよい。

【００４９】図３に本発明のホームサーバの機能ブロックを示す。本発明のホームサーバは、ＴＣＰ／ＩＰ通信制御部３－１、遠隔メソッド通信機能部３－２、暗号通信機能部３－３、カード制御機能部３－４及び電子取引管理機能部３－５より構成される。本発明で新規に追加された機能部は、暗号通信機能部３－３、カード制御機

能部３－４及び電子取引管理機能部３－５であり、それらは以下に述べる機能を備える。

【００５０】暗号通信機能部３－３は、制御通信暗号化機能３－３１、共通鍵交換代行機能３－３２及び暗号セッション管理機能３－３３を備える。カード制御機能部３－４は、ホームカード制御機能３－４１、遠隔カード制御機能３－４２及び公開鍵管理機能３－４３を備える。電子取引管理機能部３－５は、電子マネー管理機能３－５１及び決裁情報通知機能３－５２を備える。

【００５１】図４に本発明のホームカードの機能ブロックを示す。本発明のホームカードは、セキュリティ制御部４－１、プログラム実行環境設定部４－２、外部通信機能部４－３、暗号化情報管理部４－４、電子マネー管理部４－５より構成される。本発明で新規に追加される機能部は、暗号化情報管理部４－４及び電子マネー管理部４－５あり、それらは以下に述べる機能を備える。

【００５２】暗号化情報管理部４－４は、暗号アルゴリズム処理機能４－４１、電子署名機能４－４２、電子署名認証機能４－４３、証明書認証機能４－４４及び公開鍵管理機能４－４５を備える。電子マネー管理部４－５は、電子マネー制御機能４－５１及び決裁情報記録機能４－５２を備える。

【００５３】図５に本発明のアクセスカードの機能ブロックを示す。本発明のアクセスカードは、セキュリティ制御部５－１、プログラム実行環境設定部５－２、外部通信機能部５－３、ホームアクセス機能部５－４、端末プロファイル制御部５－５により構成される。本発明で新規に追加される機能部は、ホームアクセス機能部５－４及び端末プロファイル制御機能部５－５であり、それらは以下に述べる機能を備える。

【００５４】ホームアクセス機能部５－４は、暗号アルゴリズム処理機能５－４１、暗号通信機能５－４２及びホーム通信機能５－４３を備える。端末プロファイル制御部５－５は、プロファイル制御機能５－５１及び端末マンマシンインタフェース（ＭＭＩ）制御機能５－５２を備える。

【００５５】図６に本発明のホームカードセキュリティ制御手順を示す。ホームカードは、通常ハードウェア的にアクセス禁止状態にあり（ステップ６－１）、ユーザが書き換え可能なパスワードである第１のパーソナル識別番号（ＰＩＮ１）の入力があると（ステップ６－２）、該第１パーソナル識別番号（ＰＩＮ１）が正規なものかどうかを判定し（ステップ６－３）、正規なものである場合は、遠隔アクセス待状態に遷移する（ステップ６－４）。前記第１パーソナル識別番号（ＰＩＮ１）の判定（ステップ６－３）において、入力された識別番号が規定回数（例えば３回）続けて誤っていた場合、カード使用不可状態とする（ステップ６－５）。

【００５６】遠隔アクセス待状態の後、アクセスカードとの間に暗号化された制御通信を開始し（ステップ６－６）、第２のパーソナル識別番号（ＰＩＮ２）を受信すると（ステップ６－７）、該第２パーソナル識別番号（ＰＩＮ２）が正規なものであるかを判定する（ステップ６－８）。該判定において、入力された識別番号が規定回数（例えば３回）続けて誤っていた場合は、カード使用不可状態とする（ステップ６－５）。

【００５７】正規の第２パーソナル識別番号（ＰＩＮ２）を受信した場合、暗号化処理可能状態に遷移する（ステップ６－９）。暗号化処理可能状態に遷移すると、ホームカード内の暗号化情報管理部４－４が起動される（ステップ６－１０）。この状態で前述の電子商取引等における暗号化・復号化処理及び署名・証明書認証等に関する処理を実行し、ユーザから操作終了が通知されるか、又は一定期間（例えば１０分間）アクセスがない場合は操作終了と判定し（ステップ６－１１）、遠隔アクセス待状態に遷移する（ステップ６－４）。

【００５８】図７に本発明のアクセスカードによるアクセス制御手順を示す。アクセスカードは、パスワードとしてユーザが書き換え可能なパーソナル識別番号（ＰＩＮ）又はバイオ認証によりアクセス制御を行う。ここで、バイオ認証とは、指紋、声紋、虹彩又は筆跡等による本人確認の処理である。

【００５９】アクセスカードは、通常ハードウェア論理回路によりアクセス禁止状態にあり（ステップ７－１）、ユーザからのパーソナル識別番号（ＰＩＮ）入力又はバイオ認証入力があると（ステップ７－２）、該パーソナル識別番号（ＰＩＮ）又はバイオ認証入力が正規なものかどうかを判定し（ステップ７－３）、正規なものである場合は、アクセス可能状態に遷移する（ステップ７－４）。前記パーソナル識別番号（ＰＩＮ１）の判定（ステップ７－３）において、入力された識別番号が、規定回数（例えば３回）続けて誤っていた場合、カード使用不可状態とする（ステップ７－５）。

【００６０】アクセス可能状態に遷移すると、端末プロファイル制御部５－５を起動し（ステップ７－５）、ユーザ端末機器からのアクセス操作を有効にする。その後、ユーザから操作終了が通知されるか、又は一定期間（例えば１０分間）アクセス操作が行われない場合は、操作終了と判定し（ステップ７－６）、アクセス禁止状態（ステップ７－１）に遷移する。

【００６１】図８にユーザ端末機器の操作画面の一例を示す。同図の（Ａ）は無線携帯電話機、同図の（Ｂ）は携帯情報端末（ＰＤＡ）等の操作画面を示している。これらのユーザ端末機器の操作画面は、アクセスカードの端末プロファイル制御部５－５の機能により、ユーザ端末機器の種別に適した表示画面及び入力操作画面が選択され表示される。

【００６２】図９に本発明の制御通信用暗号化手順を示す。携帯端末等のユーザ端末機器では、アクセスカード内の秘密鍵及び乱数発生機能により、暗号通信開始の前

処理として電子署名を作成しておく（ステップ９－１）。ユーザ端末機器とホームサーバとの間の暗号化された制御通信の確立のため、アクセスカードのホーム通信機能５－４３とホームサーバの遠隔カード制御機能３－４２とにより通信路を確立し（ステップ９－１）、アクセスカードの暗号通信機能５－４２より、先の電子署名をホームサーバの制御通信暗号化機能３－３１へ通知し（ステップ９－３）、クライアント認証及び共通鍵の生成の基礎となる乱数を安全にホームサーバに通知する。これにより、ユーザのアクセスカードとホームサーバとの間で、共通鍵Ｘ´を用いた暗号アルゴリズムによる暗号化された制御通信が可能となる（ステップ９－４）。

【００６３】図１０に本発明のデータ通信用暗号化手順を示す。また、図１１に共通鍵交換代行の処理手順を示す。ユーザ端末機器のアクセスカードとホームサーバとの間では、前述の共通鍵Ｘ´による暗号化された制御通信が可能な状態となっている（ステップ１０－１）。

【００６４】ホームサーバは、ユーザ端末機器から電子マーケットサーバへのアクセス要求を受信すると、電子マーケットサーバに対して共通鍵交換代行処理を実行する。共通鍵交換代行処理では、電子マーケットサーバとの通信路を確立し（ステップ１０－２）、ホームカード内に格納されている秘密鍵とユーザの証明書を用いて、暗号化ハンドシェークを行い（ステップ１０－３）、ホームサーバと電子マーケットサーバとの間の共通鍵Ｘの交換を行う（ステップ１０－４）。

【００６５】ホームサーバは、電子マーケットサーバと交換した共通鍵Ｘを、ユーザ端末機器とホームサーバとの間の共通鍵Ｘ´で暗号化して通知する（ステップ１０－５）。ユーザ端末機器はホームサーバから通知された共通鍵Ｘを用いて、電子マーケットサーバとの間で暗号化されたデータ通信を行う（ステップ１０－６）。

【００６６】前述の共通鍵交換代行処理は図１１に示すように、ホームサーバが電子マーケットサーバと通信路を確立し（ステップ１１－１）、ホームカード内に格納されている秘密鍵とユーザの証明書を用いて、サーバ認証（ステップ１１－２）及びクライアント（ユーザ）認証（ステップ１１－３）の後に、電子マーケットサーバから通知（ステップ１１－４）される共通鍵Ｘの情報を、ユーザ端末機器に共通鍵Ｘ´で暗号化して通知する（ステップ１１－５）。

【００６７】図１２に本発明のアクセスカード暗号通信前処理の手順を示す。暗号化通信前処理は、電子商取引等の暗号化通信を行う前の非通信状態の任意の時間に、ユーザからの指示により起動され（ステップ１２－１）、アクセスカードの暗号通信機能が作動する（ステップ１２－２）。該暗号通信機能は乱数を発生し（ステップ１２－３）、アクセスカード内の秘密鍵及び該乱数による暗号アルゴリズムを用い（ステップ１２－４）、暗号通信開始の前処理として電子署名を作成する（ステップ１２－５）。

【００６８】この暗号アルゴリズムによる電子署名の作成は、通信開始前の前処理であるので通信料が課金されることなく、また、アクセスカードとホームサーバとの間で共通鍵Ｘ´の交換のために１回のみ行えばよいので、処理時間の遅延はそれほど気にならず、低速で演算処理を行うことが可能である。

【００６９】図１３に本発明の制御通信処理手順を示す。ユーザのアクセスカード内のアクセス機能により、宛て先固定でセットアップ（ＳＥＴＵＰ）通知がホームサーバに送信される（ステップ１３－１）。ユーザ端末機器とホームサーバ間で通信路が確立すると（ステップ１３－２）、前述の暗号通信前処理により作成しておいた電子署名を、ユーザ端末機器からホームサーバに向けて通知し、暗号通信を開始する（ステップ１３－３）。

【００７０】ホームサーバはユーザ認証を行った後、暗号通信応答を返送し（ステップ１３－４）、ユーザ端末機器とホームサーバとの間で暗号化された制御通信が開始される（ステップ１３－５）。制御通信開始後、ユーザ端末機器からホームカードのセキュリティを解放するパーソナル識別番号（ＰＩＮ２）を通知すると（ステップ１３－６）、ホームカード内のプログラムよりホームサーバ内の代行機能を起動する（ステップ１３－７）。

【００７１】図１４に本発明のホームカード遠隔操作処理手順を示す。制御通信開始（ステップ１４－１）を契機に、ホームサーバからホームカードに対して制御通信開始を通知する（ステップ１４－２）。その後、ユーザ端末機器からホームカードのセキュリティを開放するパーソナル識別番号（ＰＩＮ２）を通知すると（ステップ１４－３）、ホームカード内のプログラムで該パーソナル識別番号（ＰＩＮ２）を認証し（ステップ１４－４）、ホームカードからホームサーバの共通鍵交換代行機能を起動する（ステップ１４－５）。この状態で、ホームサーバの代行プログラムは、暗号化通信開始を監視している状態となる（ステップ１４－６）。

【００７２】図１５に本発明によるユーザから１セッションの電子マーケットへのアクセス手順を示す。電子マーケットＡのサーバとの間で、暗号化セッション（例：ｈｔｔｐｓ）を確立する場合、ユーザ端末機器から送信された暗号化セッション開始要求（ステップ１５－１）をホームサーバの代行プログラムが感知し、ホームサーバは、電子マーケットＡのサーバとの間で、暗号化通信に必要な共通鍵交換を代行する（ステップ１５－２）。

【００７３】電子マーケットＡのサーバより共通鍵Ａが通知されると（ステップ１５－３）、ホームサーバは、ユーザ端末機器に共通鍵Ａを通知する（ステップ１５－４）と共に、ホームサーバ内の暗号セッション管理部の機能を用いて、セッション番号と共通鍵情報とを格納する。ユーザ端末機器は、ホームサーバから通知された共

通鍵Ａを用い、電子マーケットサーバとの間で暗号通信を開始する（ステップ１５－５）。

【００７４】図１６に本発明によるユーザから複数セッションの電子マーケットへのアクセス手順を示す。今、ユーザ端末機器と電子マーケットＢのサーバとの間で、前述の図１５に示した手順により暗号化通信を行っている場合、ユーザ端末機器から、以前に暗号化通信を行った電子マーケットＡへの暗号化セッション（例：ｈｔｔｐｓ）確立の要求があると（ステップ１６－１）、ホームサーバは、暗号セッション管理部に格納されたセッション番号及び共通鍵情報を参照し、電子マーケットＡのサーバに対して共通鍵交換を再度行うことなく、暗号セッション管理部に格納された共通鍵Ａをユーザ端末機器に送信し（ステップ１６－２）、ユーザ端末機器は該共通鍵Ａによる電子マーケットＡのサーバとの暗号化通信を行う（ステップ１６－３）。

【００７５】図１７に本発明による電子マネー料金徴収手順を示す。電子マネーは、ホームカード内に格納されている。ユーザ端末機器から商品等を注文し（ステップ１７－１）、電子マーケットサーバから料金徴収がユーザ端末機器に通知されると（ステップ１７－２）、ユーザ端末機器は、ホームカードに対して電子マネー要求を発行する（ステップ１７－３）。

【００７６】ホームカードは、カード内に格納された電子マネーから徴収料金を減算し、電子マネー管理銀行の共通鍵とユーザの秘密鍵を使った電子署名を付与した電子マネー応答をユーザ端末機器に送信し（ステップ１７－４）、ユーザ端末機器で決済を行った電子マネー決済を電子マーケットサーバに通知する（ステップ１７－５）。

【００７７】図１８に本発明の電子マネー再補充手順を示す。ユーザ端末機器より銀行サーバに対して、ホームカードへの電子マネー再補充要求を送信する（ステップ１８－１）。該要求を受けた銀行サーバは、銀行サーバの秘密鍵とユーザの公開鍵とを使った電子署名を付与した電子マネー補充を通知する（ステップ１８－２）。

【００７８】ユーザ端末機器は、該通知された電子マネーを電子署名と共にホームカードに通知し、該電子マネーをホームカードに加算する（ステップ１８－３）。ホームカードは該電子マネー加算に対する応答をユーザ端末機器に送信し（ステップ１８－４）、ユーザ端末機器は、該電子マネー加算応答の受信により、銀行サーバに対して電子マネー再補充応答を送信する（ステップ１８－５）。銀行サーバは該電子マネー再補充応答の受信によりユーザの銀行口座に対する決済を行う（ステップ１８－６）。

【００７９】図１９に本発明の決裁情報自動通知処理手順を示す。ユーザ端末機器からホームカードに電子マネー要求を行うと（ステップ１９－１）、ホームカードから該要求に対する電子マネー応答を電子署名と共にユーザ端末機器に返送し（ステップ１９－２）、ユーザ端末機器は、該電子マネー応答により、電子マーケットサーバに対して電子マネー決済を電子署名と共に送信する（ステップ１９－３）。

【００８０】上記のようにユーザ端末機器からホームカードによる決済が行われると、ホームカードは決裁情報を自動記録し、定期的にユーザ指定のメールアドレスに対して決裁情報を通知する（ステップ１９－４）。これにより、ユーザはホームカードの不正使用等による不当な決済を素早く察知することが可能となる。

【００８１】図２０に本発明の決裁内容取り消し処理手順を示す。前述のように、ホームカードから決裁情報が自動的にユーザ指定のメールアドレスに通知され（ステップ２０－１）、該通知から一定期間以内（例えば７日以内）に、ユーザ端末機器から決裁取り消し通知を電子署名と共に電子マーケットサーバに通知すると（ステップ２０－２）、電子マーケットサーバは、該ユーザ端末機器に対して決済取り消し確認を電子署名と共に送信し（ステップ２０－３）、ユーザ端末機器は、該決済取り消し確認の受信により、当該決済で支払われた電子マネーを再度ホームカードに加算する指令を電子署名と共にホームカードに送信する（ステップ２０－３）。

【００８２】図２１に本発明の無線網での利用形態を示す。データ処理・演算処理等の処理能力の低い小型の携帯用ユーザ端末機器２１－１を使用し、該携帯用ユーザ端末機器２１－１にアクセスカード２１－２を接続し、携帯用ユーザ端末機器２１－１から無線網を介してホーム網内のホームサーバ２１－３にアクセスし、該ホームサーバ２１－３の認証・暗号化代行処理機能を利用して、電子商取引等の個人情報又は秘密情報を、電子マーケット網の電子商店サーバ２１－４又は銀行サーバ２１－５等と安全に流通することが可能となり、ユーザは、いつでもどこからでも安全性の高い電子商取引等を行うことが可能となる。また、利用結果は、ユーザ指定のメールアドレスへ通知される。

【００８３】図２２に本発明の職場等のオフィスでの利用形態を示す。職場等のオフィスに備えられ、インターネットに接続可能なコンピュータ２２－１を使用し、該コンピュータ２２－１にアクセスカード２２－２を接続してユーザのホーム網内のホームサーバ２２－３にアクセスし、該コンピュータ２２－１とホームサーバ２２－３との間でインターネットを介する暗号化通信パスにより、ホームサーバ２２－３の認証・暗号化代行処理を利用して、電子商店サーバ２２－４又は銀行サーバ２２－５に対し、電子商取引等の個人情報又は秘密情報を安全に送受することが可能となる。

【００８４】また、電子商取引以外にも、ホームサーバ２２－３に接続された家庭内の電気・電子機器の遠隔制御やそれらの機器からの情報収集等を暗号化して送受信することにより、家庭内の電気・電子機器の遠隔制御等

を安全に行うことが可能となる。

【００８５】図２３に本発明のコンビニエンスストア等での利用形態を示す。コンビニエンスストア等の商店のキャッシュレジスタやＰＯＳ（point of sales）端末等のデータ処理装置２３－１を利用し、該データ処理装置２３－１にアクセスカード２３－２を挿入し、インターネットを介してホーム網内のホームサーバ２３－３にアクセスし、ホームサーバ２３－３の認証・暗号化代行処理を利用して電子商取引に関する情報を送受することにより、安全な電子マネーの運用が可能となる。

【００８６】なお、アクセスカードが盗難され又は紛失するようなことがあっても、電子マネー及びユーザ個人の電子証明書は、セキュリティの保たれたホームサーバのホームカード内に格納されているため、電子マネー及びユーザ個人の電子証明書がアクセスカード自体から第三者により不正に利用されることはない。

【００８７】図２４に本発明の情報蓄積媒体としての利用形態を示す。ホームサーバ２４－４上で、電子手帳等の個人情報管理用ソフトウェア（ＰＩＭ）のデータ情報を管理し、アクセスカード２４－３により接続されるユーザ端末機器２４－１や公衆電話機２４－２とホームサーバ２４－４との間で、個人情報管理用ソフトウェア（ＰＩＭ）のデータ情報を同期させることにより、スケジュール管理や住所録や作業予定リスト等の個人情報を安全に蓄積し、且つ安全に読出し及び書込みができる蓄積媒体としてホームサーバ２４－４を利用することができる。

【００８８】以上、本発明による認証代行用のサーバは、限られた特定の携帯端末に対して認証を代行するだけなので、該特定の携帯端末の識別情報を記憶しておき、携帯端末からのアクセスに対して、その識別情報が記憶されているか否かを判定し、更にはそれに加えて若干の認証手順を付加することにより、携帯端末に対する認証を、従来の電子商取引等の通信相手のサーバよる認証よりも簡易な手順で済ませることができる。

【００８９】また、本発明の実施形態では、認証代行用のサーバが、電子商取引等の通信相手のサーバと所定の手順に従った全ての通信を行って認証を代行する実施形態について説明したが、認証代行用のサーバは、所定の手順に従った通信のうち一部の通信を代行し、例えば、認証手順の最初から途中までを認証代行用のサーバにより行い、その途中結果を携帯端末に送信し、以降の認証手順の通信を携帯端末とその通信相手先サーバとの間で行う構成とすることもできる。

【００９０】ただし、認証代行用のサーバによる上述の簡易認証又は一部認証は、携帯端末における認証のための全通信量又は処理負担量が、通信相手サーバと直接認証処理を行った場合に要する通信量又は処理負担量を上回らないようにすべきである。

【００９１】また、本発明の実施形態として、認証による通信相手の正当性の判定結果により、相互に秘密キーを交換する実施形態を主に説明したが、認証処理は必ずしも秘密キーを交換するためだけに行われるものではなく、認証の詰果によって他の情報を取得するといった利用形態等にも本発明を同様に適用することができる。

【００９２】（付記１）ユーザ端末機器からアクセスされ、該アクセスの際に送信される電子署名を確認し、該ユーザ端末機器との間で暗号化された通信セッションを確立する手段を備えたサーバであって、公開鍵及び秘密鍵を用い、認証処理を経て共通鍵を交換し、該共通鍵により暗号化通信を行う電子マーケットサーバ等の他のサーバに対して、該認証処理及び共通鍵の交換処理を、前記ユーザ端末機器に代わって行う認証・暗号化処理代行手段と、前記電子マーケットサーバ等の他のサーバと交換した共通鍵を、前記ユーザ端末機器に暗号化された通信セッションを介して通知する手段と、を備えたことを特徴とすると認証・暗号化処理代行サーバ。

（付記２）前記認証・暗号化処理代行サーバは、電子商取引を行うための電子署名機能及び認証機能を含む暗号化管理手段を備えたホームカードを格納し、前記電子マーケットサーバ等の他のサーバに対する認証処理及び共通鍵の交換処理を、該ホームカードの暗号化管理手段により実行することを特徴とする付記１に記載の認証・暗号化処理代行サーバ。

（付記３）　前記ホームカードは、前記ユーザ端末機器からの第１のパスワード入力によりアクセスを可能にする論理回路を備え、該アクセスを許可したユーザ端末機器との間に暗号化された通信セッションを確立した後に、該ユーザ端末機器から入力される第２のパスワードにより、前記認証・暗号化処理代行手段のセキュリティを解放する手段を備えたことを特徴とする付記２に記載の認証・暗号化処理代行サーバ。

（付記４）　前記ホームカードは、該ホームカード内の電子マネーにより決済された決裁情報を記録し、該記録した決済情報を所定のメールアドレス宛てに通知する手段を備えたことを特徴とする付記２に記載の認証・暗号化処理代行サーバ。

（付記５）　前記ホームカードは、該ホームカード内の電子マネーによる決済処理に対して、該決済処理の取り消しの認証情報に基づいて該決裁情報を取り消すと共に、該決済処理により減算された電子マネーを、ホームカード内の電子マネーに加算する手段を備えたことを特徴とする付記４に記載の認証・暗号化処理代行サーバ。

（付記６）　前記ホームカードは、前記ユーザ端末機器から要求された電子マネーの再補充要求に対して、銀行サーバ等の電子マネー管理サーバの認証情報に基づいて、要求された補充額を該ホームカードの電子マネーに加算し、再補充する手段を備えたことを特徴とする付記２に記載の認証・暗号化処理代行サーバ。

（付記７）　ユーザ端末機器に接続されるアクセスカー

ドであって、認証・暗号化処理代行機能を備えたサーバとの間に、暗号化された通信セッションを確立する手段と、前記認証・暗号化処理代行機能を備えたサーバが電子マーケットサーバ等の他のサーバに対して認証処理後に交換した共通鍵を、前記暗号化された通信セッションを介して受信し、該受信した共通鍵を用いて該電子マーケットサーバ等の他のサーバとの暗号化通信を行う手段と、を備えたことを特徴とするアクセスカード。

（付記８）　携帯端末の認証を該携帯端末との間で所定の手順に従った通信により行う認証機能を備えた種々のサーバと通信可能なサーバにおいて、該携帯端末から該携帯端末の識別情報及び認証代行処理依頼信号を受信する受信手段と、該識別情報が内部メモリ又は外部メモリに記憶されているか否か判定する判定手段と、前記判定によりメモリに記憶されており、かつ、前記所定の手順に従った通信より簡易な認証を該携帯端末との通信により行い、該携帯端末が正当であると判定した場合に、前記所定の手順に従った通信の一部又は全部を該携帯端末に代わって行う代行手段と、を備えたことを特徴とするサーバ。

（付記９）　携帯端末の認証を該携帯端末との間で所定の手順に従った通信により行う認証機能を備えた種々のサーバと通信可能なサーバ用のプログラムを記憶した記録媒体において、該携帯端末から該携帯端末の識別情報及び認証代行処理依頼信号を受信するステップと、該識別情報が内部メモリ又は外部メモリに記憶されているか否か判定するステップと、前記判定によりメモリに記憶されており、かつ、前記所定の手順に従った通信より簡易な認証を該携帯端末との通信により行い、該携帯端末が正当であると判定した場合に、前記所定の手順に従った通信の一部又は全部を該携帯端末に代わって行うステップと、をサーバが実効するためのプログラムを記憶した記録媒体。

（付記１０）　所定の手順に従った通信により通信相手の認証を行い、認証の結果、正当な通信相手であると判定した場合に、該通信相手との暗号化通信を行う際に使用する秘密情報を、該通信相手に対して送信する機能を備えた種々のサーバと通信可能な携帯端末において、自端末の識別情報及び認証代行処理依頼信号を所定のサーバに対して送信する送信手段と、該所定のサーバが該携帯端末に代わって前記通信を行い、取得した秘密情報を該所定のサーバから受信する受信手段と、を備えたことを特徴とする携帯端末。

（付記１１）　付記１０に記載の携帯端末において、前記所定のサーバに対応して秘密情報を記憶する手段と、該秘密情報を用いて前記所定のサーバと暗号化通信を行う機能を更に備え、前記所定のサーバからの前記秘密情報の受信は、該暗号化通信により受信することを特徴とする携帯端末。

【００９３】

【発明の効果】以上説明したように、本発明は、ホームサーバ等のサーバに、電子商取引等における認証及び共通鍵の交換を含む暗号化通信の前処理を代行する認証代行機能を具備させ、ユーザはユーザ端末機器からアクセスカードを用いて該サーバにアクセスし、該サーバにより認証及び共通鍵の交換を含む暗号化通信の前処理を高速に行うようにしたことにより、電子商取引等における個人情報又は秘密情報及び認証情報の送受に際して、それらのセキュリティ管理のために行われる共通鍵の交換を含む暗号化通信の前処理が短時間で行われ、ユーザの待ち時間が短縮されるとともに通信料金が節減される。

【００９４】また、前記個人情報等を格納するサーバは、セキュリティの確保された例えば家庭内等に固定的に設置され、ユーザ端末機器から該サーバにアクセスカードによってアクセスすることにより、電子商取引等における個人情報又は秘密情報及び認証情報の流失を防ぎ、不正利用に対するセキュリティ性を高めると共に、ユーザ端末機器を用いた電子商取引等の情報流通が簡便にかつ安全に行われる。

【図面の簡単な説明】

【図１】本発明による認証・暗号化代行処理システムの構成を示す図である。

【図２】本発明による認証・暗号化代行処理手順を示す図である。

【図３】本発明のホームサーバの機能ブロックを示す図である。

【図４】本発明のホームカードの機能ブロックを示す図である。

【図５】本発明のアクセスカードの機能ブロックを示す図である。

【図６】本発明のホームカードセキュリティ制御手順を示す図である。

【図７】本発明のアクセスカードによるアクセス制御手順を示す図である。

【図８】ユーザ端末機器の操作画面の一例を示す図である。

【図９】本発明の制御通信用暗号化手順を示す図である。

【図１０】本発明のデータ通信用暗号化手順を示す図である。

【図１１】本発明の共通鍵交換代行処理手順を示す図である。

【図１２】本発明のアクセスカード暗号通信前処理の手順を示す図である。

【図１３】本発明の制御通信処理手順を示す図である。

【図１４】本発明のホームカード遠隔操作処理手順を示す図である。

【図１５】本発明によるユーザから１セッションの電子マーケットへのアクセス手順を示す図である。

【図１６】本発明によるユーザから複数セッションの電

子マーケットへのアクセス手順を示す図である。

【図１７】本発明による電子マネー料金徴収手順を示す図である。

【図１８】本発明の電子マネー再補充手順を示す図である。

【図１９】本発明の決裁情報自動通知処理手順を示す図である。

【図２０】本発明の決裁内容取り消し処理手順を示す図である。

【図２１】本発明の無線網での利用形態を示す図である。

【図２２】本発明の職場等のオフィスでの利用形態を示す図である。

【図２３】本発明のコンビニエンスストア等での利用形態を示す図である。

【図２４】本発明の情報蓄積媒体としての利用形態を示す図である。

【図２５】電子商取引等における情報流通に使用されるユーザ端末機器及び情報処理装置の例を示す図である。

【図２６】従来の電子商取引等におけるセキュリティ管理技術を示す図である。

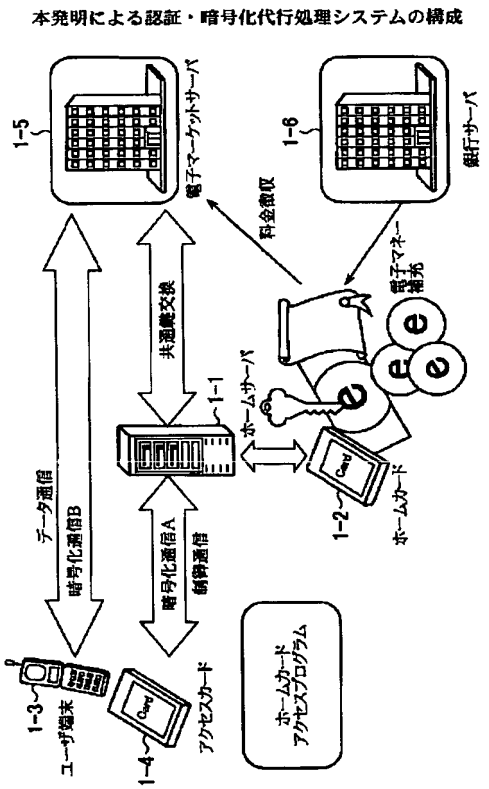
【図２７】従来のセキュリティ管理の通信手順を示す図である。

【図２８】複数の電子マーケットと電子商取引を行う様子を示す図である。

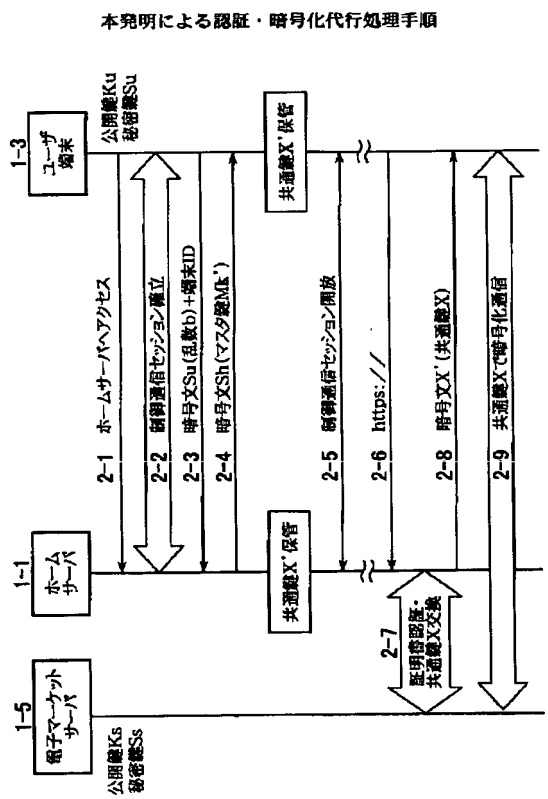
【符号の説明】

１－１　ホームサーバ
１－２　ホームカード
１－３　ユーザ端末機器
１－４　アクセスカード
１－５　電子マーケットサーバ
１－６　銀行業務用サーバ

【図１】

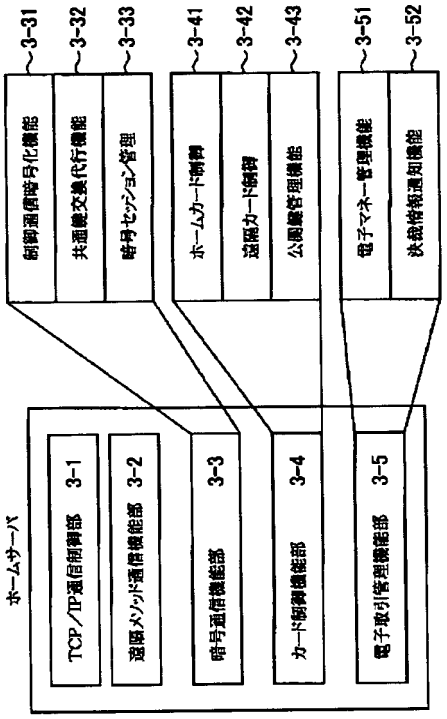


【図２】



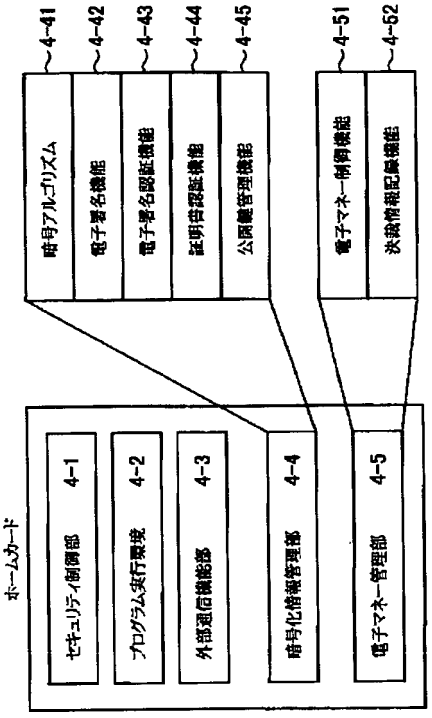
【図３】

本発明のホームサーバの機能ブロック



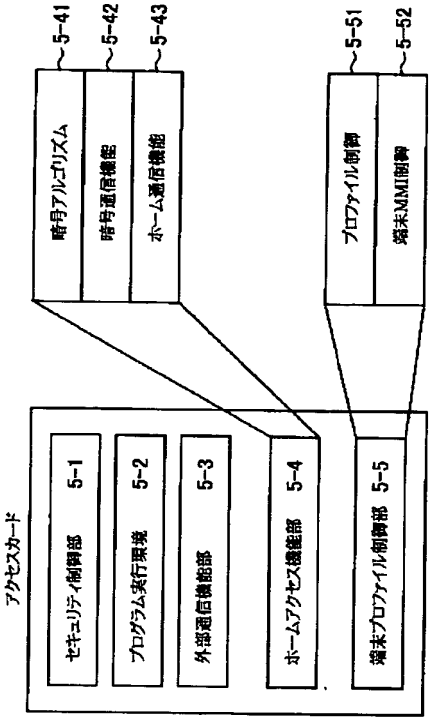
【図４】

本発明のホームカードの機能ブロック



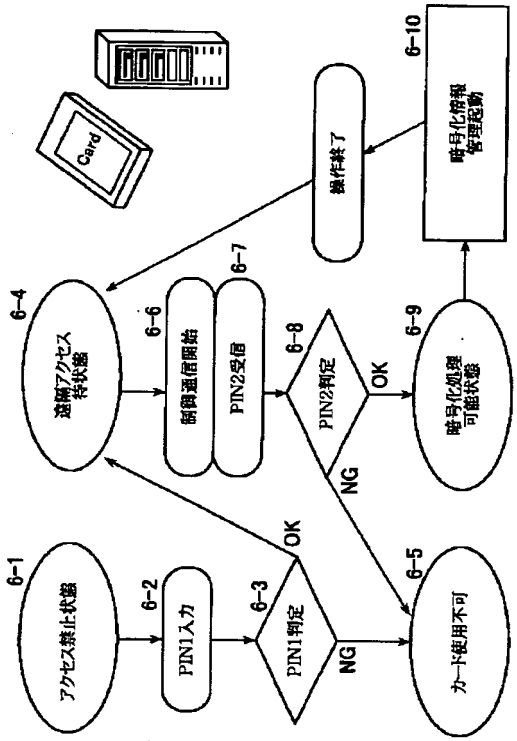
【図５】

本発明のアクセスカードの機能ブロック



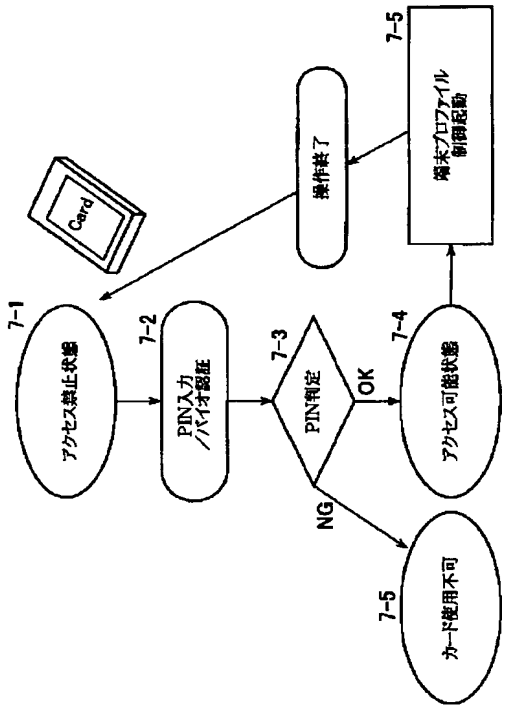
【図６】

本発明のホームカードセキュリティ制御手順



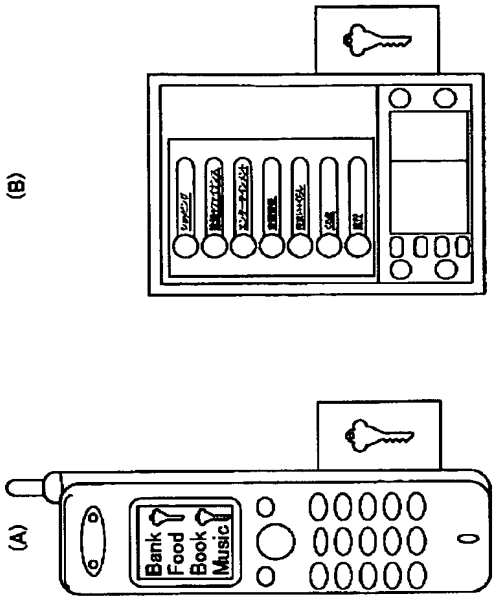
【図７】

本発明のアクセスカードによるアクセス制御手順



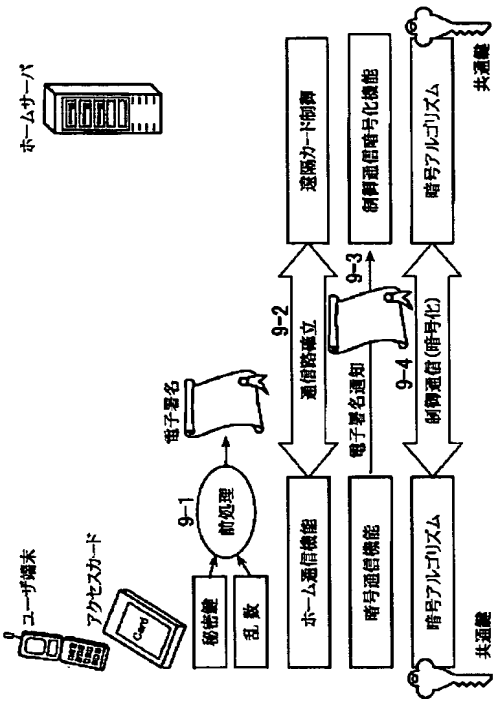
【図８】

ユーザ端末機器の操作画面の一例



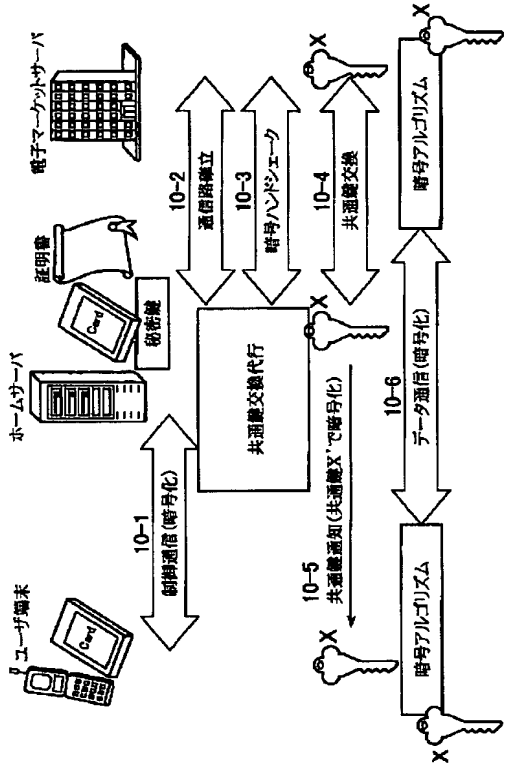
【図９】

本発明の制御通信用暗号化手順



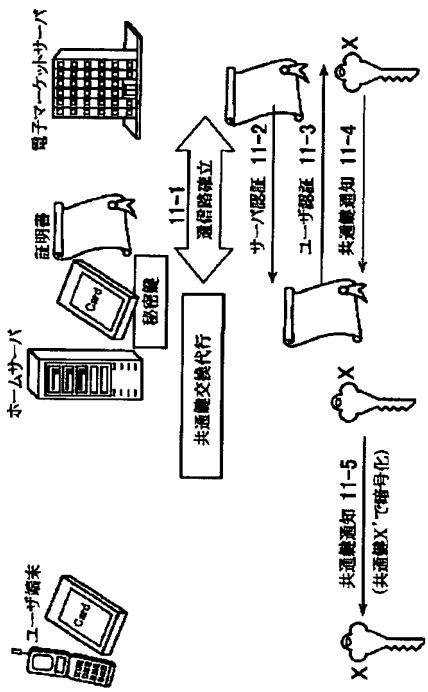
【図１０】

本発明のデータ通信用暗号化手順



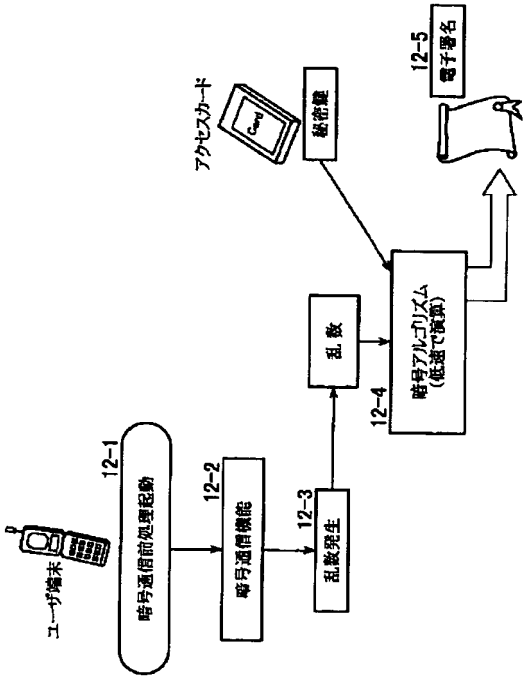
【図１１】

本発明の共通鍵交換代行処理手順



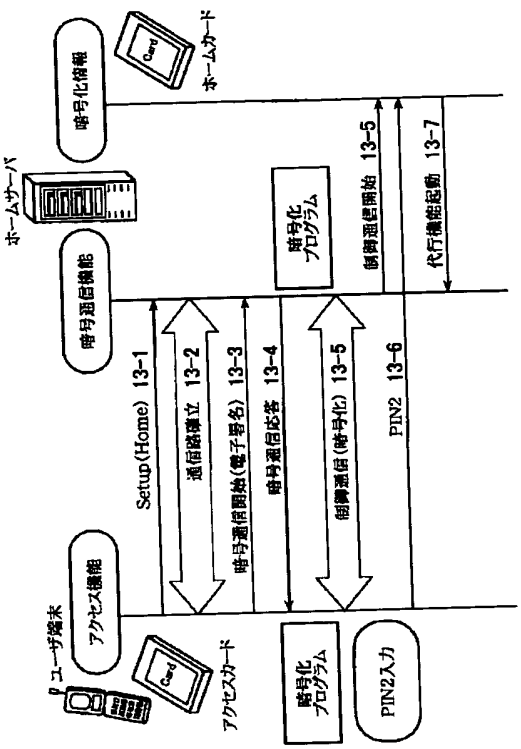
【図１２】

本発明のアクセスカード暗号通信前処理の手順



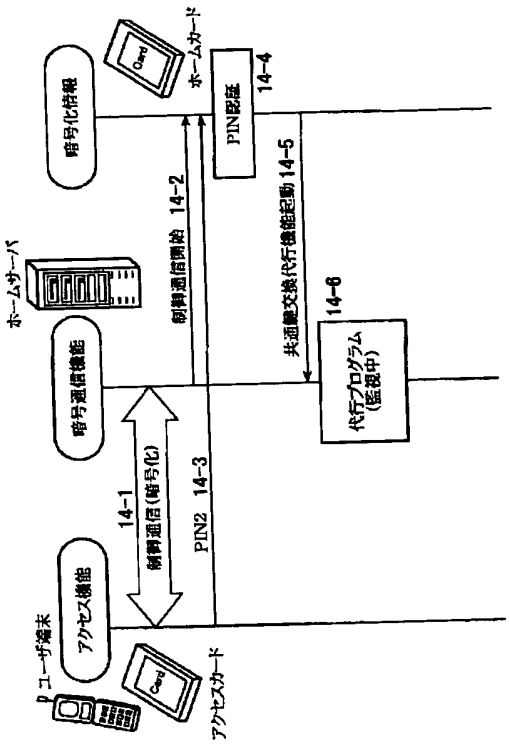
【図１３】

本発明の制御通信処理手順



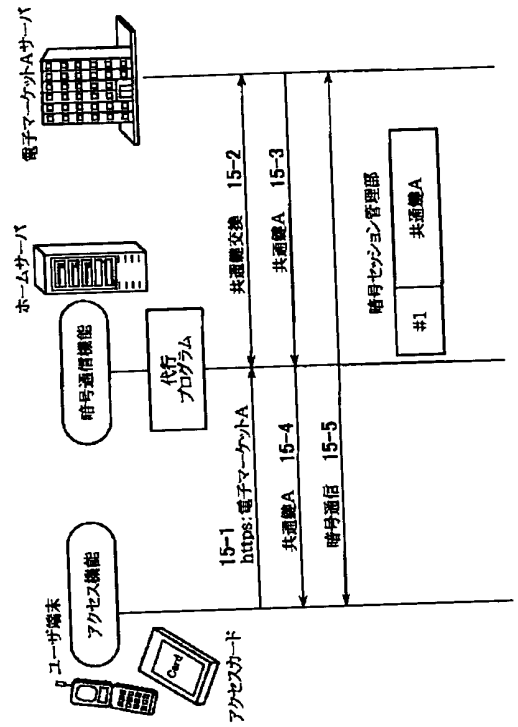
【図１４】

本発明のホームカード遠隔操作処理手順



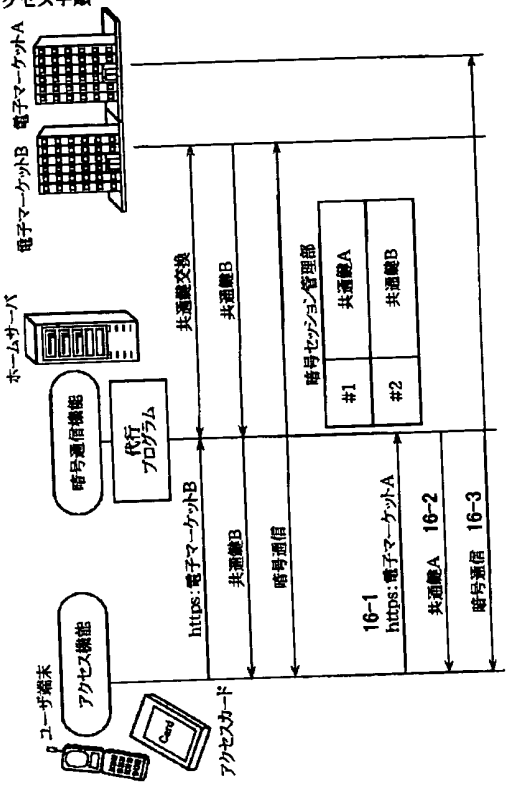
【図１５】

本発明によるユーザから１セッションの電子マーケットへのアクセス手順



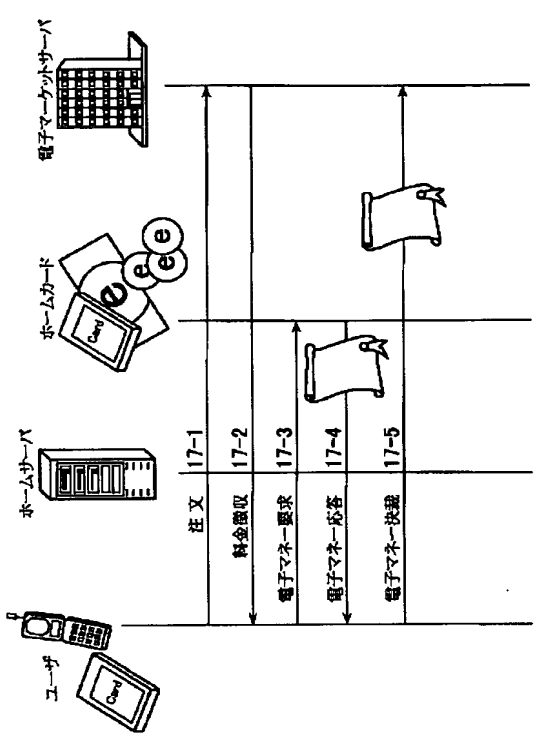
【図１６】

本発明によるユーザから複数セッションの電子マーケットへのアクセス手順



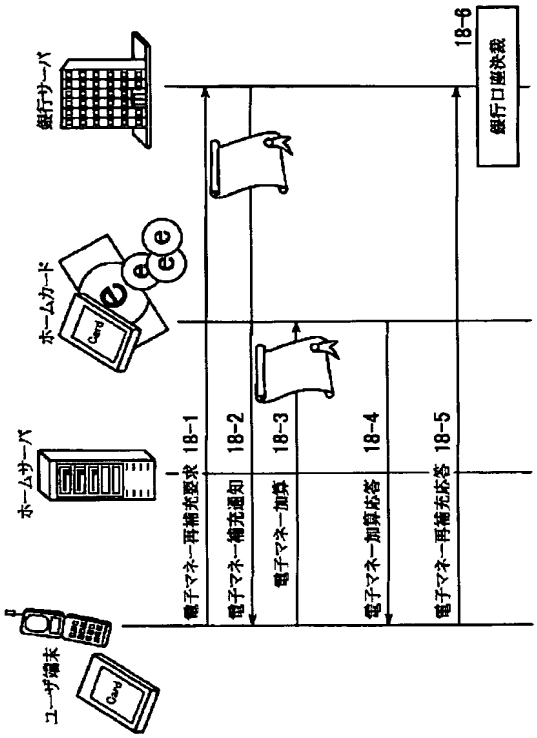
【図１７】

本発明による電子マネー料金徴収手順

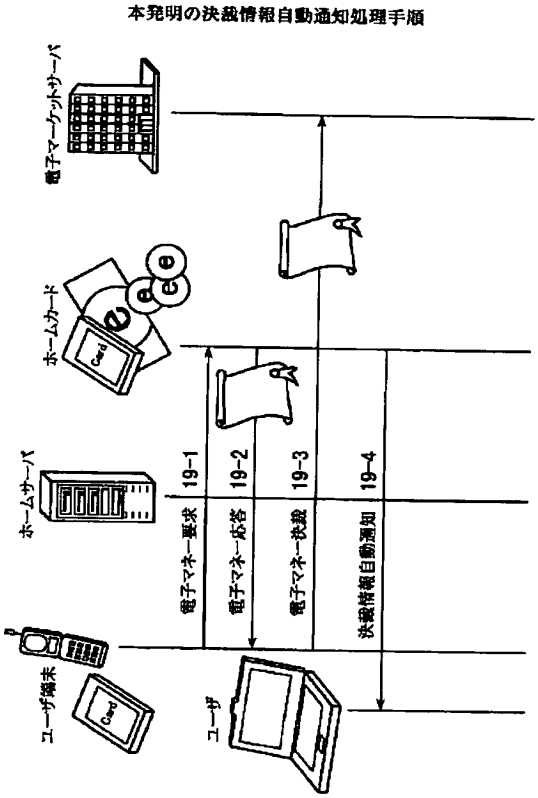


【図１８】

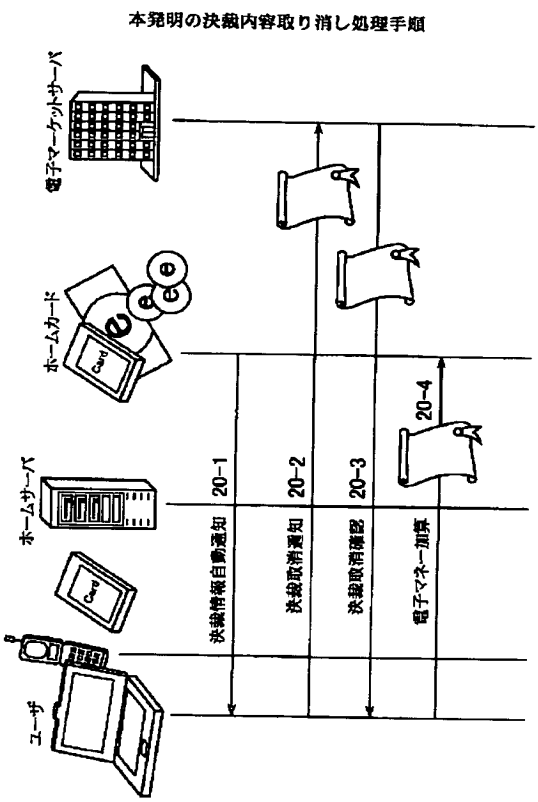
本発明の電子マネー再補充手順



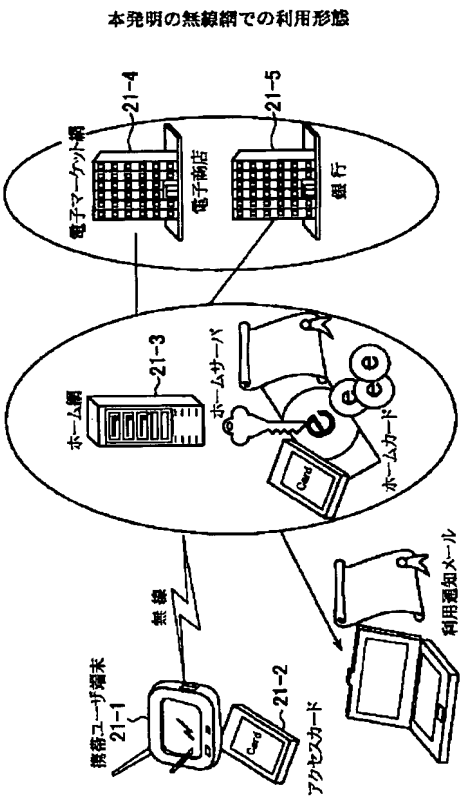
【図１９】


本発明の決裁情報自動通知処理手順
電子マーケットサーバ
ホームカード
ホームサーバ
ユーザ端末
ユーザ
19-1
19-2
19-3
19-4
電子マネー要求
電子マネー応答
電子マネー決裁
決裁情報自動通知

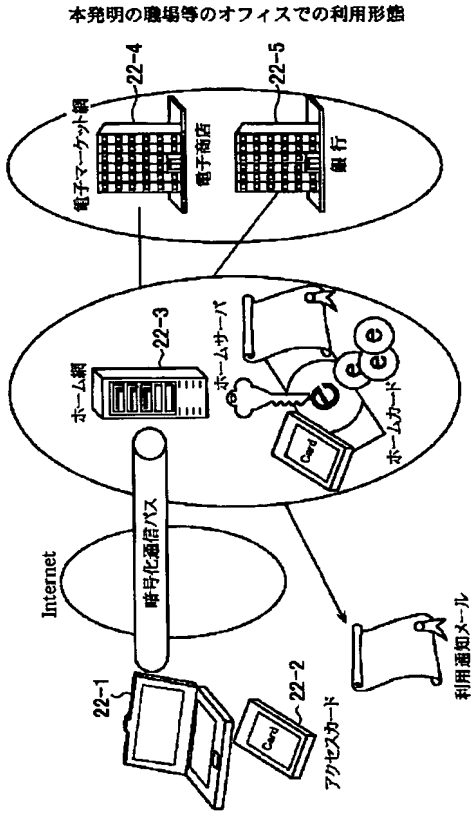
【図２０】


本発明の決裁内容取り消し処理手順
電子マーケットサーバ
ホームカード
ホームサーバ
ユーザ
20-1
20-2
20-3
20-4
決裁情報自動通知
決裁取消通知
決裁取消確認
電子マネー加算

【図２１】

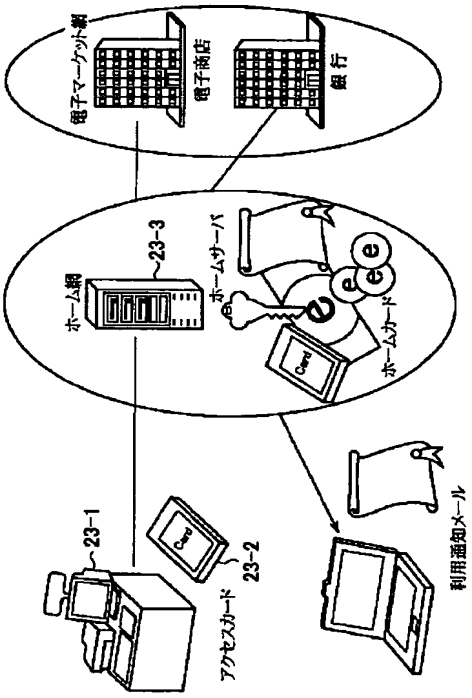

本発明の無線網での利用形態
電子マーケット網
21-4
電子商店
21-5
銀行
ホーム網
21-3
ホームサーバ
ホームカード
無線
利用通知メール
携帯ユーザ端末
21-1
21-2
アクセスカード

【図２２】


本発明の職場等のオフィスでの利用形態
電子マーケット網
22-4
電子商店
22-5
銀行
ホーム網
22-3
ホームサーバ
ホームカード
Internet
暗号化通信パス
利用通知メール
22-1
22-2
アクセスカード

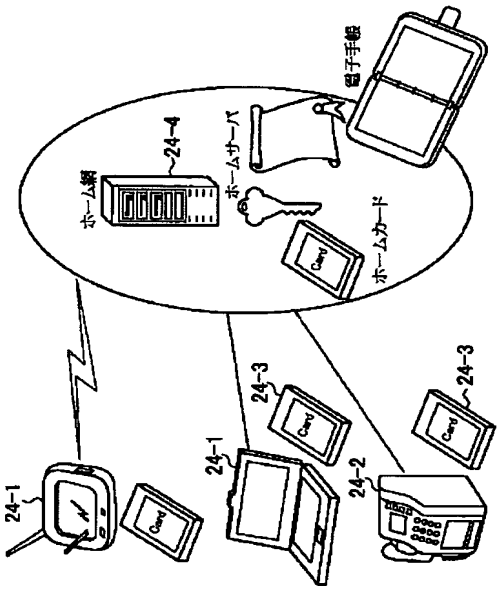
【図２３】

本発明のコンビニエンスストア等での利用形態



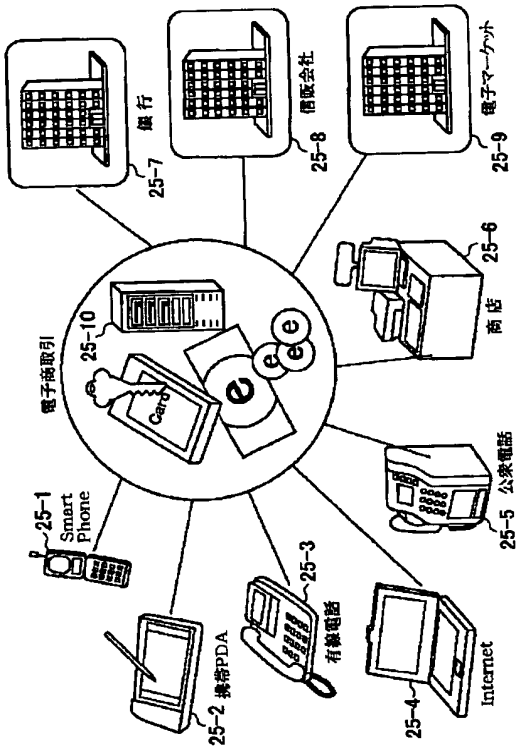
【図２４】

本発明の情報蓄積媒体としての利用形態



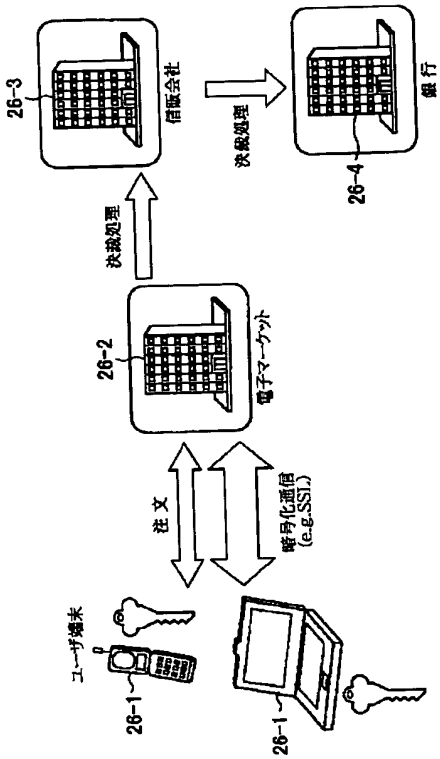
【図２５】

電子商取引等における情報流通に使用されるユーザ端末機器及び情報処理装置の例

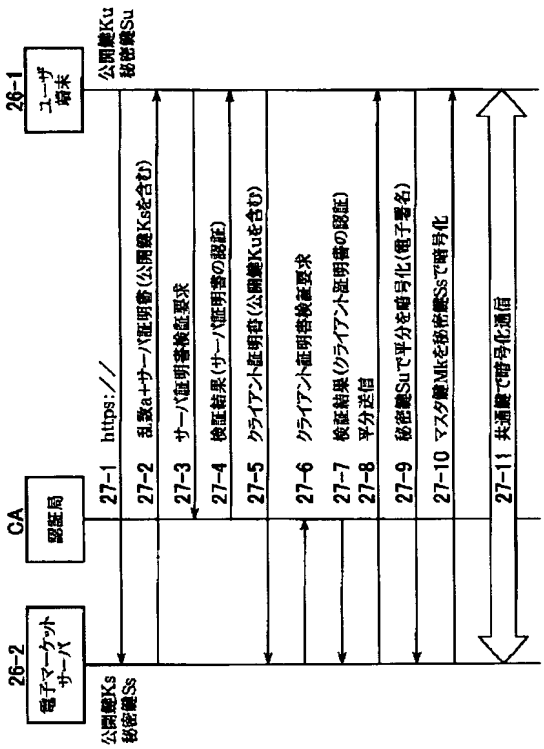


【図２６】

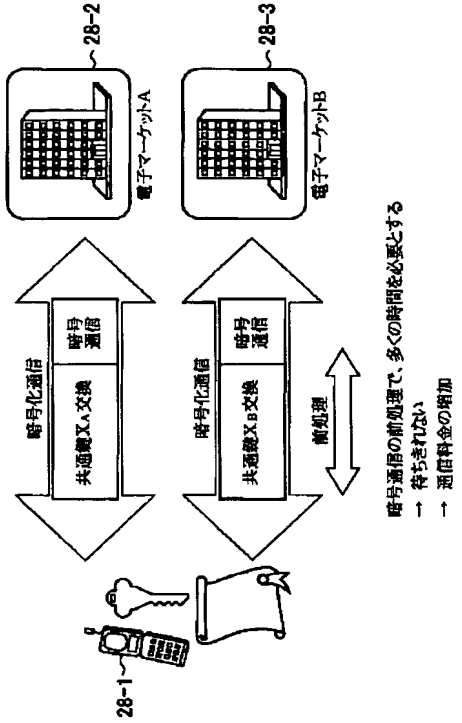
従来の電子商取引等におけるセキュリティ管理技術



【図２７】



【図２８】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/00		６０１Ｅ	
		６７５Ａ	